The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Amr Talkbox -- Amr Talkbox	** DISPUTED ** PHP remote file inclusion vulnerability in talkbox.php in Amr Talkbox allows remote attackers to execute arbitrary PHP code via a URL in the direct parameter. NOTE: this issue has been disputed by CVE, since the $direct variable is set to a static value just before the include statement.	unknown 2006-06-15	7.0	CVE-2006-3040 BUGTRAQ
Arantius -- Vice Stats	SQL injection vulnerability in vs_resource.php in Arantius Vice Stats 0.5b and 1.0 allows remote attackers to execute arbitrary SQL commands via the ID parameter.	unknown 2006-06-12	7.0	CVE-2006-2972 BUGTRAQ BID SECUNIA OTHER-REF MLIST
Arantius -- Vice Stats	SQL injection vulnerability in vs_search.php in Arantius Vice Stats before 1.0.1 allows remote attackers to execute arbitrary SQL commands via unknown vectors, a different issue than CVE-2006-2972.	unknown 2006-06-12	7.0	CVE-2006-2981 OTHER-REF MLIST
Blue-Collar -- i-Gallery	Multiple cross-site scripting (XSS) vulnerabilities in BlueCollar i-Gallery 4.1 PLUS and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) n and (2) d parameters in (a) login.asp and the d parameter in (b) igallery.asp.	unknown 2006-06-15	7.0	CVE-2006-3021 BLOGSPOT FRSIRT SECUNIA XF
Cescripts -- Event Registration 2checkout Cescripts -- Event Registration corporate Cescripts -- Event Registration RSVP Cescripts -- Event Registration paypal	Cross-site scripting (XSS) vulnerability in Event Registration allows remote attackers to inject arbitrary web script or HTML via the (1) event_id parameter to view-event-details.php or (2) select_events parameter to event-registration.php. NOTE: the provenance of this information is unknown; the details are obtained from third party information.	unknown 2006-06-16	7.0	CVE-2006-3052 FRSIRT SECUNIA
Codewalkers -- ltwCalendar	** DISPUTED ** PHP remote file inclusion vulnerability in Ltwcalendar/calendar.php in Codewalkers Ltwcalendar 4.1.3 allows remote attackers to execute arbitrary PHP code via a URL in the ltw_config[include_dir] parameter. NOTE: CVE disputes this claim, since the $ltw_config[include_dir] variable is defined as a static value in an include file before it is referenced in an include() statement.	unknown 2006-06-15	7.0	CVE-2006-3041 BUGTRAQ MLIST
Coppermine -- Photo Gallery	Unspecified vulnerability in usermgr.php in Coppermine Photo Gallery before 1.4.7 has unknown impact and remote attack vectors, possibly related to authorization/authentication errors.	unknown 2006-06-12	7.0	CVE-2006-2976 OTHER-REF OTHER-REF FRSIRT SECUNIA
Enterprise Payroll Systems -- Enterprise Payroll Systems	Multiple PHP remote file inclusion vulnerabilities in Enterprise Timesheet and Payroll Systems (EPS) 1.1 and earlier allow remote attackers to execute arbitrary PHP code via a URL in the absolutepath parameter in (1) footer.php and (2) admin/footer.php.	unknown 2006-06-12	7.0	CVE-2006-2982 OTHER-REF FRSIRT SECUNIA BID SECTRACK
Enterprise Payroll Systems -- Enterprise Payroll Systems	PHP remote file inclusion vulnerability in Enterprise Timesheet and Payroll Systems (EPS) 1.1 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the absolutepath parameter in cal.php. NOTE: the provenance of this information is unknown; the details are obtained solely from	unknown 2006-06-12	7.0	CVE-2006-2983 FRSIRT

	third party information.			
fipsASP -- fipsGallery	Cross-site scripting (XSS) vulnerability in zoom.php in fipsGallery 1.5 and earlier allows remote attackers to inject arbitrary web script or HTML via the path parameter.	unknown 2006-06-15	7.0	CVE-2006-3022 BLOGSPOT FRSIRT SECUNIA
Foing -- Foing	PHP remote file inclusion vulnerability in manage_songs.php in Foing 0.7.0e and earlier allows remote attackers to execute arbitrary PHP code via a URL in the foing_root_path parameter.	unknown 2006-06-16	7.0	CVE-2006-3045 BUGTRAQ
Horde -- Horde	Cross-site scripting (XSS) vulnerability in horde 3 (horde3) before 3.1.1 allows remote attackers to inject arbitrary web script or HTML via unknown vectors.	unknown 2006-06-15	7.0	CVE-2006-2195 DEBIAN
ISPConfig -- ISPConfig	Multiple PHP remote file inclusion vulnerabilities in ISPConfig 2.2.3 allow remote attackers to execute arbitrary PHP code via a URL in the (1) go_info[isp][classes_root] parameter in (a) server.inc.php, and the (2) go_info[server][classes_root] parameter in (b) app.inc.php, (c) login.php, and (d) trylogin.php.	unknown 2006-06-15	7.0	CVE-2006-3042 BUGTRAQ
Lucid Designs -- Lucid Calendar	Cross-site scripting (XSS) vulnerability in Cal.PHP3 in Chris Lea Lucid Calendar 0.22 allows remote attackers to inject arbitrary web script or HTML via unspecified parameters. NOTE: the provenance of this information is unknown; the details are obtained from third party information.	unknown 2006-06-15	7.0	CVE-2006-3025 BID
Mafia Moblog -- Mafia Moblog	SQL injection vulnerability in big.php in Mafia Moblog 0.6M1 and earlier allows remote attackers to execute arbitrary SQL commands via the img parameter.	unknown 2006-06-12	7.0	CVE-2006-2977 BUGTRAQ SECUNIA FRSIRT BID
Microsoft -- Windows Media Player	Stack-based buffer overflow in Microsoft Windows Media Player 9 and 10 allows remote attackers to execute arbitrary code via a PNG image with a large chunk size.	2006-02-22 2006-06-13	7.0	CVE-2006-0025 IDEFENSE MS BID FRSIRT SECUNIA CERT CERT-VN SECTRACK
Microsoft -- Internet Explorer	Unspecified vulnerability in Microsoft Internet Explorer 5.01 SP4 and 6 SP1 and earlier allows remote attackers to execute arbitrary code by instantiating certain COM objects from Wmm2fxa.dll as ActiveX controls, which causes memory corruption.	unknown 2006-06-13	7.0	CVE-2006-1303 MS BID FRSIRT SECTRACK SECUNIA
Microsoft -- Windows ME Microsoft -- Windows 98 Microsoft -- Windows 2000 Microsoft -- Windows Server 2003 Microsoft -- Windows XP	Microsoft JScript 5.1, 5.5, and 5.6 on Windows 2000 SP4, and 5.6 on Windows XP, Server 2003, Windows 98 and Windows Me, will "release objects early" in certain cases, which results in memory corruption and allows remote attackers to execute arbitrary code.	unknown 2006-06-13	7.0	CVE-2006-1313 MS CERT-VN BID FRSIRT SECUNIA CERT SECTRACK
Microsoft -- Windows 2000 Microsoft -- Windows Server 2003 Microsoft -- Windows XP	The Server Message Block (SMB) driver (MRXSMB.SYS) in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 SP1 and earlier allows local users to execute arbitrary code by calling the MrxSmbCscIoctlOpenForCopyChunk function with the METHOD_NEITHER method flag and an arbitrary address, possibly for kernel memory, aka the "SMB Driver Elevation of Privilege Vulnerability."	2005-12-09 2006-06-13	10.0	CVE-2006-2373 IDEFENSE MS BID FRSIRT SECUNIA
Microsoft -- Windows 98 Microsoft -- Windows ME	Heap-based buffer overflow in the PolyPolygon function in Graphics Rendering Engine on Microsoft Windows 98 and Me allows remote attackers to execute arbitrary code via a crafted Windows Metafile (WMF) or EMF image.	unknown 2006-06-13	7.0	CVE-2006-2376 MS BID BUGTRAQ FRSIRT SECUNIA CERT CERT-VN SECTRACK
Microsoft -- Internet Explorer	Unspecified vulnerability in Microsoft Internet Explorer 5.01 SP4 and 6 SP1 and earlier allows remote attackers to execute arbitrary code via "unexpected data" related to "parameter validation" in the DXImageTransform.Microsoft.Light ActiveX control, which causes Internet Explorer to crash in a way that enables the code execution.	2006-06-13 2006-06-13	7.0	CVE-2006-2383 MS CERT-VN BID FRSIRT CERT

				SECTRACK SECUNIA
MyBB -- MyBB	The domecode function in inc/functions_post.php in MyBulletinBoard (MyBB) 1.1.2, and possibly other versions, allows remote attackers to execute arbitrary PHP code via the username field, which is used in a preg_replace function call with a /e (executable) modifier.	2006-06-06 2006-06-12	7.0	CVE-2006-2908 BUGTRAQ OTHER-REF FRSIRT SECUNIA BID OSVDB SECTRACK
NPDS -- NPDS	Multiple cross-site scripting (XSS) vulnerabilities in Net Portal Dynamic System (NPDS) 5.10 and earlier allow remote attackers to inject arbitrary web script and HTML via the (1) Titlesitename or (2) sitename parameter to (a) header.php, (3) nuke_url parameter to (b) meta/meta.php, (4) forum parameter to (c) viewforum.php, (5) post_id, (6) forum, (7) topic, or (8) arbre parameter to (d) editpost.php, or (9) uname or (10) email parameter to (e) user.php.	2006-06-08 2006-06-12	7.0	CVE-2006-2951 BUGTRAQ OTHER-REF FRSIRT SECUNIA BID OSVDB OSVDB OSVDB OSVDB
Particle Soft -- Particle Links	SQL injection vulnerability in index.php in Particle Links 1.2.2 allows remote attackers to execute arbitrary SQL commands via the topic parameter.	unknown 2006-06-13	7.0	CVE-2006-3008 BUGTRAQ BID SECUNIA
Phorum -- Phorum	PHP remote file inclusion vulnerability in common.php in PHORUM 5.1.13 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the PHORUM[http_path] parameter.	unknown 2006-06-16	7.0	CVE-2006-3053 BUGTRAQ BID XF
PHP Group -- PHP	Unspecified vulnerability in session.c in PHP before 5.1.3 has unknown impact and attack vectors, related to "certain characters in session names," including special characters that are frequently associated with CRLF injection, SQL injection, and cross-site scripting (XSS) vulnerabilities. NOTE: while the nature of the vulnerability is unspecified, it is likely that this is related to a violation of an expectation by PHP applications that the session name is alphanumeric, as implied in the PHP manual for session_name().	unknown 2006-06-14	7.0	CVE-2006-3016 OTHER-REF OSVDB SECUNIA
PHP Lite -- Calendar Express	Multiple SQL injection vulnerabilities in month.php in PHP Lite Calendar Express 2.2 allow remote attackers to execute arbitrary SQL commands via the (1) catid and (2) cid parameter.	unknown 2006-06-12	7.0	CVE-2006-2973 BUGTRAQ BID FRSIRT
PicoZip -- PicoZip	Stack-based buffer overflow in the info tip shell extension (zipinfo.dll) in PicoZip 4.01 allows remote attackers to execute arbitrary code via a long filename in an (1) ACE, (2) RAR, or (3) ZIP archive, which is triggered when the user moves the mouse over the archive.	2006-06-06 2006-06-16	7.0	CVE-2006-2909 BUGTRAQ OTHER-REF OTHER-REF BID FRSIRT SECUNIA
Planete Afrique -- WS-Album	Multiple cross-site scripting (XSS) vulnerabilities in FullPhoto.asp in WS-Album 1.1 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) image and (2) PublisedDate parameters.	unknown 2006-06-15	7.0	CVE-2006-3020 BLOGSPOT MLIST FRSIRT SECUNIA XF
Tikiwiki Project -- Tikiwiki	SQL injection vulnerability in TikiWiki 1.9.3.2 and possibly earlier versions allows remote attackers to execute arbitrary SQL commands via unknown attack vectors.	unknown 2006-06-16	7.0	CVE-2006-3048 BUGTRAQ SECUNIA
VBZooM -- VBZooM	Multiple SQL injection vulnerabilities in VBZooM 1.11 allow remote attackers to execute arbitrary SQL commands via the (1) sobjectID or (2) MAINID parameters to (a) show.php or (3) MainID parameter to (b) subject.php.	unknown 2006-06-16	7.0	CVE-2006-3054 BUGTRAQ BUGTRAQ BID
VBZooM -- VBZooM	Multiple SQL injection vulnerabilities in VBZooM 1.02 allow remote attackers to execute arbitrary SQL commands via the (1) QuranID, (2) ShowByQuranID, or (3) Action parameters to meaning.php.	unknown 2006-06-16	7.0	CVE-2006-3055 BUGTRAQ BID
VBZooM -- VBZooM	SQL injection vulnerability in language.php in VBZooM 1.01 allows remote attackers to execute arbitrary SQL commands via the Action parameter.	unknown 2006-06-16	7.0	CVE-2006-3056 BUGTRAQ BID

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Aliacom -- Open Business Management	Multiple cross-site scripting (XSS) vulnerabilities in Open Business Management (OBM) 1.0.3 pl1 allow remote attackers to inject arbitrary HTML or web script via the (1) tf_lang, (2) tf_name, (3) tf_user, (4) tf_lastname, (5) tf_contact, (6) tf_datebefore, and (7) tf_dateafter parameters to files such as (a) publication/publication_index.php, (b) group/group_index.php, (c) user/user_index.php, (d) list/list_index.php, and (e) company/company_index.php.	2006-06-07 2006-06-13	4.7	CVE-2006-3009 BID OSVDB OSVDB OSVDB OSVDB OSVDB SECUNIA XF
Aliacom -- Open Business Management	Multiple SQL injection vulnerabilities in Open Business Management (OBM) 1.0.3 pl1 allow remote attackers to execute arbitrary SQL commands via the (1) new_order and (2) order_dir parameters to (a) index.php, (b) group/group_index.php, (c) user/user_index.php, (d) list/list_index.php, and (e) company/company_index.php, and the (3) entity and (4) tf_dateafter parameter to company/company_index.php.	2006-06-06 2006-06-13	4.7	CVE-2006-3010 BID OSVDB OSVDB OSVDB OSVDB OSVDB SECUNIA XF
Andy Mack -- 35mmslidegallery	Multiple cross-site scripting (XSS) vulnerabilities in 35mmslidegallery 6.0 allow remote attackers to inject arbitrary web script or HTML via the (1) imgdir parameter in (a) index.php, and the (2) w, (3) h, and (4) t parameters in (b) popup.php.	2006-06-13 2006-06-15	4.7	CVE-2006-3036 BUGTRAQ BID
Chemical Dictionary -- Chemical Dictionary	Cross-site scripting (XSS) vulnerability in dictionary.php in Chemical Dictionary allows remote attackers to inject arbitrary web script or HTML via the keyword parameter in a browse action.	2006-06-08 2006-06-12	4.7	CVE-2006-2988 BUGTRAQ FRSIRT SECUNIA BID
Christian Becher -- phazizGuestbook	Multiple cross-site scripting (XSS) vulnerabilities in index.php in phazizGuestbook 2.0 allow remote attackers to inject arbitrary web script or HTML via the (1) name, (2) email, (3) url, and (4) text fields.	2006-06-08 2006-06-12	4.7	CVE-2006-2994 BUGTRAQ
ClickGallery -- ClickGallery	Multiple cross-site scripting (XSS) vulnerabilities in ClickGallery 5.0 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) gallery_id parameter in gallery.asp and (2) parentcurrentpage parameter in view_gallery.asp.	2006-06-09 2006-06-15	4.7	CVE-2006-3026 OTHER-REF FRSIRT SECUNIA
ClickTech -- Clickcart	Cross-site scripting (XSS) vulnerability in default.asp in ClickTech Clickcart 6.0 and earlier allows remote attackers to inject arbitrary web script or HTML via the cat parameter.	2006-06-09 2006-06-15	4.7	CVE-2006-3029 OTHER-REF FRSIRT SECUNIA XF
Debian -- wv2	Integer overflow in wv2 before 0.2.2 might allow context-dependent attackers to execute arbitrary code via a crafted Microsoft Word document.	unknown 2006-06-15	4.2	CVE-2006-2197 DEBIAN
Dominios Europa -- PICRATE	Multiple SQL injection vulnerabilities in Dominios Europa PICRATE (aka TAL RateMyPic) 1.0 allow remote attackers to execute arbitrary SQL commands via the (1) id, (2) voteid, and (3) vfiel parameters to (a) index.php, and via the (4) nick, (5) email, (6) city, (7) messen, and (8) message form field parameters to (b) add.php. NOTE: the provenance of this information is unknown; the details are obtained from third party information.	2006-06-02 2006-06-12	4.7	CVE-2006-2987 FRSIRT SECUNIA
DwZone -- DwZone Shopping Cart	Multiple cross-site scripting (XSS) vulnerabilities in DwZone Shopping Cart 1.1.9 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) ToCategory and (2) FromCategory parameters to (a) ProductDetailsForm.asp and (3) UserName and (4) Password parameters to (b) LogIn/VerifyUserLog.asp.	2006-06-10 2006-06-15	4.7	CVE-2006-3030 OTHER-REF FRSIRT SECUNIA XF
Easy Ad-Manager -- Easy Ad-Manager	Cross-site scripting (XSS) vulnerability in details.php in Easy Ad-Manager allows remote attackers to inject arbitrary web script or HTML via the mbid parameter, which is reflected in an error message.	2006-06-08 2006-06-12	4.7	CVE-2006-3002 BUGTRAQ BID FRSIRT SECUNIA
EvGenius -- EvGenius Counter	Multiple cross-site scripting (XSS) vulnerabilities in EvGenius Counter 3.4 and earlier allow remote attackers to inject arbitrary web script or HTML via the page parameter in (1) monthly.php and (2) daily.php.	2006-06-13 2006-06-15	4.7	CVE-2006-3024 OTHER-REF FRSIRT SECUNIA
fipsASP -- fipsCMS	Multiple cross-site scripting (XSS) vulnerabilities in index.asp in fipsCMS 4.5 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) w, (2) phcat, (3) dayid, and (4) calw parameters.	2006-06-09 2006-06-15	4.7	CVE-2006-3031 OTHER-REF FRSIRT SECUNIA

free QBoard -- free QBoard	PHP remote file inclusion vulnerability in board/post.php in free QBoard 1.1 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the qb_path parameter.	2006-06-12 2006-06-12	4.7	CVE-2006-2998 OTHER-REF FRSIRT SECUNIA BID
IISWorks -- ListPics	Cross-site scripting (XSS) vulnerability in listpics.asp in ASP ListPics 4.3 and earlier allows remote attackers to inject arbitrary web script or HTML via the info parameter.	2006-06-09 2006-06-12	4.7	CVE-2006-2989 OTHER-REF SECUNIA FRSIRT
LoudHush -- LoudHush	The iax_net_read function in the iaxclient open source library, as used in multiple products including (a) LoudHush 1.3.6, (b) IDE FISK 1.35 and earlier, (c) Kiax 0.8.5 and earlier, (d) DIAX, (e) Ziaxphone, (f) IAX Phone, (g) X-lite, (h) MediaX, (i) Extreme Networks ePhone, and (j) iaxComm before 1.2.0, allows remote attackers to execute arbitrary code via crafted IAX 2 (IAX2) packets with truncated (1) full frames or (2) mini-frames, which are detected in a length check but still processed, leading to buffer overflows related to negative length values.	unknown 2006-06-09	4.7	CVE-2006-2923 OTHER-REF BID SECUNIA BUGTRAQ OTHER-REF OTHER-REF OTHER-REF FRSIRT FRSIRT FRSIRT FRSIRT SECUNIA SECUNIA SECUNIA
LoveCompass -- aePartner	PHP remote file inclusion vulnerability in inc/design.inc.php in LoveCompass aePartner 0.8.3 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the dir[data] parameter.	2006-06-10 2006-06-12	4.7	CVE-2006-2996 OTHER-REF BID SECUNIA FRSIRT
Microsoft -- PowerPoint	Unspecified vulnerability in Microsoft PowerPoint in Microsoft Office 2000 SP3, Office XP SP3, Office 2003 SP1 and SP2, Office 2004 for Mac, and v. X for Mac allows user-complicit attackers to execute arbitrary code via a PowerPoint document with a malformed record, which triggers memory corruption.	unknown 2006-06-13	5.6	CVE-2006-0022 MS CERT-VN BID FRSIRT SECUNIA CERT SECTRACK
Microsoft -- Exchange Server	Cross-site scripting (XSS) vulnerability in Microsoft Exchange Server 2000 SP1 through SP3, when running Outlook Web Access (OWA), allows user-complicit remote attackers to inject arbitrary HTML or web script via unknown vectors related to "HTML parsing."	unknown 2006-06-13	5.6	CVE-2006-1193 MS BID FRSIRT OTHER-REF CERT CERT-VN SECTRACK SECUNIA
Microsoft -- Windows 2000 Microsoft -- Windows Server 2003 Microsoft -- Windows XP	Buffer overflow in the Routing and Remote Access service (RRAS) in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 SP1 and earlier allows remote unauthenticated or authenticated attackers to execute arbitrary code via certain crafted "RPC related requests," aka the "RRAS Memory Corruption Vulnerability."	unknown 2006-06-13	4.2	CVE-2006-2370 MS BID FRSIRT CERT CERT-VN SECTRACK SECUNIA
Microsoft -- Windows 2000 Microsoft -- Windows Server 2003 Microsoft -- Windows XP	Buffer overflow in the Remote Access Connection Manager service (RASMAN) service in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 SP1 and earlier allows remote unauthenticated or authenticated attackers to execute arbitrary code via certain crafted "RPC related requests," that lead to registry corruption and stack corruption, aka the "RASMAN Registry Corruption Vulnerability."	unknown 2006-06-13	4.2	CVE-2006-2371 MS BUGTRAQ BID FRSIRT CERT CERT-VN SECTRACK SECUNIA
Microsoft -- Internet Explorer	Heap-based buffer overflow in Microsoft Internet Explorer 5.01 SP4 and 6 SP1 and earlier allows remote attackers to execute arbitrary code via crafted UTF-8 encoded HTML that results in size discrepancies during conversion to Unicode, aka "HTML Decoding Memory Corruption Vulnerability."	2006-06-13 2006-06-13	4.7	CVE-2006-2382 MS BUGTRAQ OTHER-REF CERT-VN BID FRSIRT

				CERT SECTRACK SECUNIA
Minerva -- Minerva	PHP remote file inclusion vulnerability in stat_modules/users_age/module.php in Minerva 2.0.8a Build 237 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the phpbb_root_path parameter.	2006-06-13 2006-06-15	4.7	CVE-2006-3028 OTHER-REF MLIST FRSIRT SECUNIA
My Photo Scrapbook -- My Photo Scrapbook	Cross-site scripting (XSS) vulnerability in display.asp in My Photo Scrapbook 1.0 and earlier allows remote attackers to inject arbitrary web script or HTML via the key_m parameter.	2006-06-09 2006-06-12	4.7	CVE-2006-2992 OTHER-REF FRSIRT SECUNIA
MyScrapbook -- MyScrapbook	Cross-site scripting (XSS) vulnerability in MyScrapbook 3.1 allows remote attackers to inject arbitrary web script or HTML via the input box in singlepage.php when submitting scrapbook pages.	2006-06-11 2006-06-15	4.7	CVE-2006-3033 BUGTRAQ BID SECUNIA
MyScrapbook -- MyScrapbook	Multiple cross-site scripting (XSS) vulnerabilities in addwords.php in MyScrapbook 3.1 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) name and (2) comment parameters. NOTE: the provenance of this information is unknown; the details are obtained from third party information.	2006-06-13 2006-06-15	4.7	CVE-2006-3035 FRSIRT
OkScripts -- QuickLinks	Cross-site scripting (XSS) vulnerability in search.php in OkScripts QuickLinks 1.1 allows remote attackers to inject arbitrary web script or HTML via the q parameter.	2006-06-08 2006-06-12	4.7	CVE-2006-2999 BUGTRAQ FRSIRT SECUNIA
OkScripts -- OkArticles	Cross-site scripting (XSS) vulnerability in search.php in OkScripts OkArticles 1.0 allows remote attackers to inject arbitrary web script or HTML via the q parameter.	2006-06-08 2006-06-12	4.7	CVE-2006-3000 BUGTRAQ FRSIRT SECUNIA
OkScripts -- OkMall	Cross-site scripting (XSS) vulnerability in search.php in OkScripts OkMall 1.0 allow remote attackers to inject arbitrary web script or HTML via the page parameter. NOTE: this might be resultant from another vulnerability, since the XSS is reflected in an error message.	2006-06-08 2006-06-12	4.7	CVE-2006-3001 BUGTRAQ FRSIRT SECUNIA
Pensacola Web Designs -- Xtreme ASP Photo Gallery	Multiple cross-site scripting (XSS) vulnerabilities in Xtreme ASP Photo Gallery 1.05 and earlier, and possibly 2.0 (trial), allow remote attackers to inject arbitrary web script or HTML via the (1) catname and (2) total parameters in (a) displaypic.asp, and the (3) catname parameter in (b) displaythumbs.asp.	2006-06-10 2006-06-15	4.7	CVE-2006-3032 OTHER-REF FRSIRT SECUNIA XF
PHP Group -- PHP	Unspecified vulnerability in PHP before 5.1.3 can prevent a variable from being unset even when the unset function is called, which might cause the variable's value to be used in security-relevant operations.	unknown 2006-06-14	4.9	CVE-2006-3017 OTHER-REF OSVDB SECUNIA
PHP Group -- PHP	Unspecified vulnerability in the session extension functionality in PHP before 5.1.3 has unkown impact and attack vectors related to heap corruption.	unknown 2006-06-14	4.9	CVE-2006-3018 OTHER-REF OSVDB SECUNIA
Six Offene Systeme GmbH -- SixCMS	Cross-site scripting (XSS) vulnerability in list.php in SixCMS 6.0 and earlier allows remote attackers to inject arbitrary script code or HTML via the page parameter.	unknown 2006-06-16	5.6	CVE-2006-3051 BUGTRAQ OTHER-REF BID SECTRACK
Subtext -- Subtext	Unspecified vulnerability in the admin login feature in Subtext 1.5, in a multiblog setup, allows remote administrators of one blog to login to another blog.	unknown 2006-06-16	4.2	CVE-2006-3046 OTHER-REF FRSIRT SECUNIA
Uapplication -- Uphotogallery	Multiple cross-site scripting (XSS) vulnerabilities in thumbnails.asp in Uapplication Uphotogallery 1.1 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) s and (2) block parameters.	2006-06-10 2006-06-15	4.7	CVE-2006-3023 OTHER-REF FRSIRT SECUNIA
VanillaSoft -- Helpdesk	Cross-site scripting (XSS) vulnerability in default.asp in VanillaSoft Helpdesk 2005 and earlier allows remote attackers to inject arbitrary web script or HTML via the username parameter.	2006-06-09 2006-06-12	4.7	CVE-2006-2990 OTHER-REF SECUNIA BID FRSIRT SECTRACK

WebprojectDB -- WebprojectDB	Multiple PHP remote file inclusion vulnerabilities in WebprojectDB 0.1.3 and earlier allow remote attackers to execute arbitrary PHP code via a URL in the INCDIR parameter in (1) include/nav.php and (2) include/lang.php.	2006-06-11 2006-06-12	4.7	CVE-2006-2995 OTHER-REF SECUNIA BID FRSIRT

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Baby Katie Media -- very Simple Realty Lister (vsREAL) Baby Katie Media -- very Simple Car Lister (vSCAL)	Multiple cross-site scripting (XSS) vulnerabilities in Baby Katie Media (a) very Simple Car Lister (vSCAL) 1.0 and (b) very simple Realty Lister (vsREAL) 1.0 allow remote attackers to inject arbitrary web script or HTML via the (1) lid parameter in index.php and the (2) title parameter in myslideshow.php.	unknown 2006-06-12	2.3	CVE-2006-2986 BUGTRAQ FRSIRT SECUNIA BID
Cescripts -- Realty Room Rent	Cross-site scripting (XSS) vulnerability in index.php in Cescripts Realty Room Rent allows remote attackers to inject arbitrary web script or HTML via the sel_menu parameter.	unknown 2006-06-15	1.9	CVE-2006-3038 BUGTRAQ FRSIRT SECUNIA
Cescripts -- Realty Home Rent	Cross-site scripting (XSS) vulnerability in index.php in Cescripts Realty Home Rent allows remote attackers to inject arbitrary web script or HTML via the sel_menu parameter.	unknown 2006-06-15	1.9	CVE-2006-3039 BUGTRAQ FRSIRT SECUNIA
CFXe-CMS -- CFXe-CMS	Cross-site scripting (XSS) vulnerability in search.cfm in CFXe-CMS 2.0 and earlier allows remote attackers to execute arbitrary web script or HTML via the voltext_suche parameter.	unknown 2006-06-16	1.9	CVE-2006-3043 OTHER-REF FRSIRT SECUNIA
Easy Ad-Manager -- Easy Ad-Manager	details.php in Easy Ad-Manager allows remote attackers to obtain the full installation path via an invalid mbid parameter, which leaks the path in an error message. NOTE: this might be resultant from another vulnerability, since this vector also produces cross-site scripting (XSS).	2006-06-08 2006-06-12	2.3	CVE-2006-3003 BUGTRAQ SECUNIA
EmailArchitect -- Email Server	Multiple cross-site scripting (XSS) vulnerabilities in EmailArchitect Email Server 6.1.0.5 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) errCode and (2) uid parameter in (a) default.asp and (3) dname parameter in (b) /admin/dns.asp and (c) /additional/regdomain_done.asp.	unknown 2006-06-12	1.9	CVE-2006-2974 FRSIRT SECTRACK SECUNIA
Enthrallweb -- ePhotos	Multiple SQL injection vulnerabilities in Enthrallwebe ePhotos 2.2 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) CAT_ID parameter in (a) subphotos.asp and (b) subLevel2.asp, the (2) AL_ID parameter in (c) photo.asp, and the (3) SUB_ID parameter in (d) subLevel2.asp.	unknown 2006-06-15	3.3	CVE-2006-3027 BLOGSPOT FRSIRT SECUNIA
Gentoo -- media-libs/jpeg Gentoo -- Gentoo Linux	The JPEG library in media-libs/jpeg before 6b-r7 on Gentoo Linux is built without the -maxmem feature, which could allow context-dependent attackers to cause a denial of service (memory exhaustion) via a crafted JPEG file that exceeds the intended memory limits.	unknown 2006-06-13	2.3	CVE-2006-3005 OTHER-REF GENTOO SECUNIA
GNOME -- dhcdbd	Unspecified vulnerability in NetworkManager daemon for DHCP (dhcdbd) allows remote attackers to cause a denial of service (crash) via certain invalid DHCP responses that trigger memory corruption.	unknown 2006-06-16	2.3	CVE-2006-3057 UBUNTU BID
iFoto -- iFoto	Cross-site scripting (XSS) vulnerability in iFoto 0.20, and possibly other versions before 0.50, allows remote attackers to inject arbitrary HTML or web script via a base64-encoded file parameter.	unknown 2006-06-13	2.3	CVE-2006-3006 BUGTRAQ BUGTRAQ SECUNIA BID FRSIRT
IntegraMOD -- IntegraMOD	Cross-site scripting (XSS) vulnerability in index.php in IntegraMOD 1.4.0 and earlier allows remote attackers to inject arbitrary web script or HTML via the STYLE_URL parameter. NOTE: it is possible that this issue is resultant from SQL injection.	unknown 2006-06-12	2.3	CVE-2006-2984 BUGTRAQ FRSIRT SECUNIA
KDE -- KDE	KDE Display Manager (KDM) in KDE 3.2.0 up to 3.5.3 allows local users to read arbitrary files via a symlink attack related to the session type for login.	unknown 2006-06-15	1.9	CVE-2006-2449 BUGTRAQ REDHAT UBUNTU BID
KDE -- aRts	artswrapper in aRts, when running setuid root on Linux 2.6.0 or later versions, does not check the return value of the setuid function call, which allows local users to gain root privileges by causing setuid to fail, which prevents artsd from dropping privileges.	unknown 2006-06-15	3.4	CVE-2006-2916 KDE KDE BID

L0j1k -- tinyMuw	Cross-site scripting (XSS) vulnerability in L0j1k tinyMuw 0.1.0 allow remote attackers to inject arbitrary web script or HTML via a javascript URI in the SRC attribute of an IMG element in the input box in quickchat.php, and possibly other manipulations.	unknown 2006-06-12	2.3	CVE-2006-2969 BUGTRAQ FRSIRT SECUNIA
L0j1k -- tinyMuw	videoPage.php in L0j1k tinyMuw 0.1.0 allows remote attackers to obtain sensitive information via a certain id parameter, probably with an invalid value, which reveals the path in an error message.	unknown 2006-06-12	2.3	CVE-2006-2970 BUGTRAQ FRSIRT
LogiSphere -- LogiSphere	Cross-site scripting (XSS) vulnerability in LogiSphere 1.6.0 allows remote attackers to inject arbitrary web script or HTML via the URL, which is reflected in an error page.	2006-05-16 2006-06-16	1.9	CVE-2006-3044 FRSIRT OSVDB SECTRACK SECUNIA
Mafia Moblog -- Mafia Moblog	Mafia Moblog 0.6M1 and earlier allows remote attackers to obtain the installation path in an error message via a direct request to (1) big.php and (2) upgrade.php.	unknown 2006-06-12	2.3	CVE-2006-2978 BUGTRAQ SECUNIA FRSIRT
Microsoft -- Windows 2000 Microsoft -- Windows Server 2003 Microsoft -- Windows XP	The Server Message Block (SMB) driver (MRXSMB.SYS) in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 SP1 and earlier allows local users to cause a denial of service (hang) via by calling the MrxSmbCscIoctlCloseForCopyChunk with the file handle of the shadow device, which results in a deadlock, aka the "SMB Invalid Handle Vulnerability."	unknown 2006-06-13	1.6	CVE-2006-2374 MS IDEFENSE BID FRSIRT SECUNIA
Microsoft -- Internet Explorer Microsoft -- Windows Server 2003 Microsoft -- Windows XP	Buffer overflow in the ART Image Rendering component (jgdw400.dll) in Microsoft Windows XP SP1 and Sp2, Server 2003 SP1 and earlier, and Windows 98 and Me allows remote attackers to execute arbitrary code via a crafted ART image that causes heap corruption.	unknown 2006-06-13	3.5	CVE-2006-2378 IDEFENSE MS CERT-VN BID FRSIRT SECUNIA CERT SECTRACK
Microsoft -- Windows NT Microsoft -- Windows 2000 Microsoft -- Windows Server 2003 Microsoft -- Windows XP	Buffer overflow in the TCP/IP Protocol driver in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 SP1 and earlier allows remote attackers to execute arbitrary code via unknown vectors related to IP source routing.	unknown 2006-06-13	2.3	CVE-2006-2379 MS CERT-VN BID SECUNIA CERT FRSIRT SECTRACK
Microsoft -- Windows 2000	Microsoft Windows 2000 SP4 does not properly validate an RPC server during mutual authentication over SSL, which allows remote attackers to spoof an RPC server, aka the "RPC Mutual Authentication Vulnerability."	unknown 2006-06-13	2.3	CVE-2006-2380 MS BID FRSIRT SECTRACK SECUNIA
Microsoft -- Internet Explorer	Microsoft Internet Explorer 5.01 SP4 and 6 SP1 and earlier allows remote attackers to conduct spoofing and phishing attacks by using a modal browser window in a way that preserves the original address bar and trusted UI of a trusted site, even after the browser has been navigated to a malicious site, aka the "Address Bar Spoofing Vulnerability."	unknown 2006-06-13	3.7	CVE-2006-2384 MS BID FRSIRT SECTRACK SECUNIA
Microsoft -- Internet Explorer	Unspecified vulnerability in Microsoft Internet Explorer 5.01 SP4 and 6 SP1 and earlier allows user-complicit remote attackers to execute arbitrary code via a crafted web page that triggers memory corruption when it is saved as a multipart HTML (.mht) file.	unknown 2006-06-13	3.7	CVE-2006-2385 MS BID FRSIRT SECTRACK SECUNIA
Mole Group Ticket Booking Script -- Mole Group Ticket Booking Script	Multiple cross-site scripting (XSS) vulnerabilities in booking3.php in Mole Group Ticket Booking Script allow remote attackers to inject arbitrary web script or HTML via the (1) name, (2) address1, (3) address2, (4) county, (5) postcode, (6) email, (7) phone, or (8) mobile parameters to booking2.php.	unknown 2006-06-16	2.3	CVE-2006-3049 BUGTRAQ MLIST FRSIRT SECUNIA
My Photo Scrapbook -- My Photo Scrapbook	Multiple SQL injection vulnerabilities in My Photo Scrapbook 1.0 and earlier allow remote attackers to execute arbitrary SQL commands via the key parameter in (1) Displayview.asp and (2) Details_Photo_bv.asp.	unknown 2006-06-12	2.3	CVE-2006-2993 OTHER-REF FRSIRT SECUNIA

MyScrapbook -- MyScrapbook	MyScrapbook 3.1 allows remote attackers to obtain sensitive information via a direct request to files in the txt-db-api directory such as txt-db-api/sql.php, which reveals the path in an error message.	2006-06-11 2006-06-15	2.3	CVE-2006-3034 BUGTRAQ FRSIRT SECUNIA
Net Portal Dynamic System -- Net Portal Dynamic System	Net Portal Dynamic System (NPDS) 5.10 and earlier allows remote attackers to obtain sensitive information via a direct request to (1) header.php, (2) contact.php, or (3) forum_extender.php, which reveals the path in an error message.	unknown 2006-06-12	3.5	CVE-2006-2950 BUGTRAQ OTHER-REF FRSIRT SECUNIA
Net Portal Dynamic System -- Net Portal Dynamic System	Directory traversal vulnerability in Net Portal Dynamic System (NPDS) 5.10 and earlier allows remote attackers to read arbitrary files via a .. (dot dot) sequence and trailing null (%00) byte in the (1) Default_Theme parameter to header.php or (2) ModPath parameter to modules/cluster-paradise/cluster-E.php.	unknown 2006-06-12	3.5	CVE-2006-2952 BUGTRAQ OTHER-REF FRSIRT SECUNIA BID OSVDB OSVDB
NullSoft -- Shoutcast Server	Multiple cross-site scripting (XSS) vulnerabilities in SHOUTcast 1.9.5 allow remote attackers to inject arbitrary HTML or web script via the DJ fields (1) Description, (2) URL, (3) Genre, (4) AIM, and (5) ICQ.	unknown 2006-06-13	2.3	CVE-2006-3007 BUGTRAQ BID FRSIRT SECUNIA
Overkill -- Overkill	Integer overflow in the recv_packet function in 0verkill 0.16 allows remote attackers to cause a denial of service (daemon crash) via a UDP packet with fewer than 12 bytes, which results in a long length value to the crc32 function.	unknown 2006-06-12	2.3	CVE-2006-2971 BUGTRAQ BID FRSIRT SECUNIA
PBL Guestbook -- PBL Guestbook	Multiple cross-site scripting (XSS) vulnerabilities in pblguestbook.php in PBL Guestbook 1.31 allow remote attackers to inject arbitrary web script or HTML via javascript in the SRC attribute of IMG tags in the (1) name, (2) email, and (3) website parameter, which bypasses XSS protection mechanisms that check for SCRIPT tags but not IMG. NOTE: portions of this description's details are obtained from third party information.	unknown 2006-06-12	1.9	CVE-2006-2975 BUGTRAQ FRSIRT SECUNIA
PHP -- PHP	Buffer consumption vulnerability in the tempnam function in PHP 5.1.4 and 4.x before 4.4.3 allows local users to bypass restrictions and create PHP files with fixed names in other directories via a pathname argument longer than MAXPATHLEN, which prevents a unique string from being appended to the filename.	unknown 2006-06-13	1.6	CVE-2006-2660 OTHER-REF BUGTRAQ SECTRACK
PHP Labware -- LabWiki	Cross-site scripting (XSS) vulnerability in search.php in PHP Labware LabWiki 1.0 allows remote attackers to inject arbitrary web script or HTML via the search input box (query parameter).	unknown 2006-06-12	2.3	CVE-2006-2968 BUGTRAQ MLIST BID SECTRACK
phpCMS -- phpCMS	Multiple PHP remote file inclusion vulnerabilities in phpCMS 1.2.1pl2 allow remote attackers to execute arbitrary PHP code via a URL in the PHPCMS_INCLUDEPATH parameter to files in parser/include/ including (1) class.parser_phpcms.php, (2) class.session_phpcms.php, (3) class.edit_phpcms.php, (4) class.http_indexer_phpcms.php, (5) class.cache_phpcms.php, (6) class.search_phpcms.php, (7) class.lib_indexer_universal_phpc ms.php, and (8) class.layout_phpcms.php, (9) parser/plugs/counter.php, and (10) parser/parser.php.	unknown 2006-06-15	2.3	CVE-2006-3019 BUGTRAQ FRSIRT SECUNIA
Ringlink -- Ringlink	Multiple cross-site scripting (XSS) vulnerabilities in Ringlink 3.2 allow remote attackers to inject arbitrary web script or HTML via a JavaScript URI in the SRC attribute of an IMG element, and possibly other manipulations, in the ringid parameter in (1) next.cgi, (2) stats.cgi, or (3) list.cgi.	unknown 2006-06-12	2.3	CVE-2006-2991 BUGTRAQ BID FRSIRT SECUNIA OSVDB OSVDB OSVDB
ScriptsEZ -- Ez Ringtone Manager	Multiple cross-site scripting (XSS) vulnerabilities in Ez Ringtone Manager allow remote attackers to inject arbitrary web script or HTML via the (1) id parameter in player.php and (2) keyword parameter when performing a search.	unknown 2006-06-12	2.3	CVE-2006-3004 BUGTRAQ BID FRSIRT SECUNIA
Site Trade -- ST AdManager Lite	Multiple cross-site scripting (XSS) vulnerabilities in publish.php in ST AdManager Lite allow remote attackers to inject arbitrary web script or HTML via the (1) title, (2) description, (3) article, (4) bio, and (5) name parameters.	unknown 2006-06-15	1.9	CVE-2006-3037 BUGTRAQ FRSIRT SECUNIA

Six Offene Systeme GmbH -- SixCMS	Directory traversal vulnerability in detail.php in SixCMS 6.0 and earlier allows remote attackers to read arbitrary files via a .. (dot dot) sequence and trailing null (%00) byte in the template parameter.	unknown 2006-06-16	1.9	CVE-2006-3050 BUGTRAQ OTHER-REF BID SECTRACK
Syworks -- SafeNET	Syworks SafeNET allows local users to bypass restrictions on network resource consumption by editing the policy.dat file.	2006-04-18 2006-06-12	1.6	CVE-2006-2967 BUGTRAQ SECTRACK
The Integramod Group -- IntegraMOD	SQL injection vulnerability in index.php in IntegraMOD 1.4.0 and earlier allows remote attackers to execute arbitrary SQL commands via double-encoded """ characters in the STYLE_URL parameter.	unknown 2006-06-12	2.3	CVE-2006-2985 BUGTRAQ MLIST
Tikiwiki Project -- Tikiwiki	Cross-site scripting (XSS) vulnerability in tikiwiki 1.9.3.2 and possibly earlier versions allows remote attackers to inject arbitrary web script or HTML via unknown attack vectors.	unknown 2006-06-16	2.3	CVE-2006-3047 BUGTRAQ OTHER-REF SECUNIA
ViArt -- Shop	Multiple cross-site scripting (XSS) vulnerabilities in ViArt Shop Free 2.5.5, and possibly other distributions including Light, Standard, and Enterprise, allow remote attackers to inject arbitrary web script or HTML via the (1) forum_id parameter in forum.php, which is not properly handled in block_forum_topics.php, and (2) item_id parameter in reviews.php, which is not properly handled in block_reviews.php.	2006-06-06 2006-06-12	1.9	CVE-2006-2979 BUGTRAQ OTHER-REF MLIST FRSIRT SECUNIA BID
ViArt Ltd -- ViArt Shop Free	SQL injection vulnerability in block_forum_topic_new.php in ViArt Shop Free 2.5.5, and possibly other distributions including Light, Standard, and Enterprise, might allow remote attackers to execute arbitrary SQL commands via unknown vectors, probably involving the forum_id parameter.	unknown 2006-06-12	2.3	CVE-2006-2980 MLIST OTHER-REF
WinSCP -- WinSCP	Argument injection vulnerability in WinSCP 3.8.1 build 328 allows remote attackers to upload or download arbitrary files via encoded spaces and double-quote characters in a scp or sftp URI.	2006-06-04 2006-06-14	3.7	CVE-2006-3015 FULLDISC BID FRSIRT SECUNIA
ZMS Publishing -- ZMS	Cross-site scripting (XSS) vulnerability in ZMS 2.9 and earlier, when register_globals is enabled, allows remote attackers to inject arbitrary web script or HTML via the raw parameter in the search field.	unknown 2006-06-12	2.3	CVE-2006-2997 OTHER-REF SECUNIA BUGTRAQ FRSIRT SECTRACK

Back to top

Last updated June 19, 2006